FILED
2023 Jul-19 PM 01:45
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
NORTHEASTERN DIVISION

OAKWOOD UNIVERSITY, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No.**
	)	
DYNAMIC CAMPUS SOLUTIONS, INC.,	)	
	)	
	)	
Defendant.	)	

FIRST AMENDED COMPLAINT

Oakwood University ("Oakwood" or the "University") asserts the following Complaint against Defendant Dynamic Campus Solutions, Inc. ("Dynamic Campus" or "DCS"):

Parties

1. Founded in 1898, Oakwood is a Historically Black College and University ("HBCU") in Huntsville, Alabama that is affiliated with the Seventh-day Adventist Church. Oakwood has a rich history and legacy both as an HBCU and a Church institution. Oakwood's mission is to transform students for service to God and humanity through a biblically based curriculum. Amazingly, it does so from a campus that used to be a slave plantation (an estate on which Dred Scott once

labored).[1]

2. Oakwood has consistently been ranked by the U.S. News & World Report as one of the nation's "Best Colleges" in both its HBCUs and "Regional Colleges/South" categories. Additionally, Oakwood is the nation's fifth-ranked producer of undergraduate black applicants to medical schools, according to the Association for American Medical Colleges.

3. Dynamic Campus is a corporation organized under the laws of the State of California, with a principal place of business located at 2806 Flintrock Trace, Suite A205, Austin Texas, 78738. In 2019, Dynamic Campus contracted to provide information technology (IT) services for Oakwood in Huntsville, Alabama.

4. Oakwood now is, and at all times mentioned was, a domestic non-profit corporation duly organized and existing under the laws of Alabama with its principal place of business located at 7000 Adventist Blvd. NW, Huntsville, AL 35896.

Jurisdiction and Venue

5. The Court has subject matter jurisdiction over this action and personal jurisdiction over both parties. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1332 as the parties are citizens of different states and the amount in controversy exceeds $75,000.

[1] https://www.al.com/news/huntsville/2023/02/remembering-dred-scott-an-alabama-slave-who-made-american-history.html?outputType=amp.

6. The Court has personal jurisdiction over Plaintiff, as it employed workers who provided IT services for Oakwood within the State of Alabama. Additionally, the parties entered into an Information Technology Services Agreement (the "Agreement"). By doing so, Dynamic Campus consented to this Court's jurisdiction for any lawsuit arising out of that Agreement.

7. Venue is proper in the Court under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claim occurred in Madison County. In addition, the parties' Agreement includes a Controlling Law and Venue provision, stating that any litigation will be brough in a court of competent jurisdiction over civil actions in Madison County, Alabama.

Background – The Threat of Cyberattacks

8. In our connected, data-driven society, any person or organization who uses electronic mail, social media or the internet is at risk of falling victim to a cyberattack or data breach.

9. Colleges and Universities receive and maintain large amounts of confidential data from their students, faculty, employees, and other stakeholders.

These institutions are common targets for cyberattacks. Because HBCUs are often underfunded, they seem to be enticing targets for cybercriminals.

10. One type of cyber-crime is called a "ransomware" attack. In a ransomware attack, a "Threat Actor"[2] (a/k/a "hacker" or "cyber-criminal") develops a scheme to trick an IT user into bringing ransomware into the victim's IT systems. A common example is an email asking the recipient to click on an attachment that includes ransomware. If the user falls for the trick, the ransomware ends up in the user's IT system. If the user's IT systems (and/or data on those systems) are not properly protected, the cybercriminals are able to access data and programs, lock the victims out of their systems, and ultimately, demand a ransom from the victim to regain access to their own information.

11. Ransomware attacks can cause significant operational, structural, and reputational harm to victims, even when the victim is able to pay the ransom.

Oakwood University IT Systems

12. Information technology is vital to Oakwood's operations, mission and ability to serve its students, employees, and other stakeholders.

13. Oakwood maintains several vital IT systems/programs, including

[2] "Threat actor" is defined as "a participant (person or group) in an action or process that is characterized by malice or hostile action (intending harm) using computers, devices, systems, or networks." Center for Internet Security, https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors.

electronic mail, student accounts, student records, payroll, and employee records. Needless to say, these systems maintain personal, confidential and/or proprietary information and records, all of which Oakwood needs to protect from data breaches or cyberattack.

14. Lacking the cybersecurity expertise to take these steps itself, the University has contracted with a "Managed Services Provider" to be subject matter experts for, work with, and be a part Oakwood's Information Technology Department. Dynamic Campus was one such Managed Services Provider, serving in that role from May 1, 2019, until late 2022.

Dynamic Campus

15. Dynamic Campus holds itself out to the public as a market leader in information technology outsourcing and managed services provider for private colleges and universities (like Oakwood). Dynamic Campus targets higher education customers, selling them on their expertise and experience performing cybersecurity, data retention and risk reduction.

16. Dynamic Campus promises to give its customers "peace of mind," so that they do not need to worry about the risks posed to the institutions by cyberattacks or ransomware. *See* https://dynamiccampus.com/.

17. Oakwood believed Dynamic Campus's representations and reasonably relied on Dynamic Campus to provide these vital services for Oakwood and its stakeholders.

The Parties' IT Services Agreement

18. Based on Dynamic Campus's representations, Oakwood contracted with DCS on May 1, 2019 (the "Agreement").

19. The Agreement obligated Dynamic Campus to provide services to ensure the security of Oakwood's IT Systems. Dynamic Campus agreed to assist the University in backing up its confidential, vital, and ever-changing data. Dynamic Campus agreed to maintain the backups in secure locations and generally help the University fend off and/or lessen the risks of a cyber-attack. (*See* Exhibit A, Information Technology Services Agreement at 17-18).

20. In addition to the provisions of the Agreement, Dynamic Campus owed a duty of reasonable care to Oakwood to maintain the University's data and systems in a reasonable manner, in accordance with applicable industry standards.

21. Dynamic Campus's vital services did not come cheap. In fact, Oakwood paid Dynamic Campus a huge amount for this protection (an amount exceeding $6,000,000 over three years).

22. Had Dynamic Campus simply done what it was supposed to do, their charges would have been worth it. But, as Oakwood will demonstrate, Dynamic

Campus failed to deliver on its promises and obligations, all of which caused substantial harm to Oakwood University.

The Service Agreement Kicks Off

23. In June 2019, Dynamic Campus announced that it was Oakwood's "strategic technology partner." The announcement promoting its plans to "provide Oakwood with the IT leadership and support higher education students, faculty and staff expect and require today."[3] In the announcement, Dynamic Campus touted that it would service Oakwood's IT platforms with an "on-site team [. . .] backed by [Dynamic Campus's] deep nationwide bench of higher education IT experts to ensure Oakwood's evolving technology needs are met for years to come."

24. In accordance with the Agreement, Dynamic Campus received expansive authority to supervise and manage **all** aspects of the University's technology systems. This included daily database management services. It also required Dynamic Campus to guide the University's strategic decision-making about cybersecurity, system security, data backup, and disaster recovery needs. (Exhibit A at 15-16).

[3] Dynamic Campus, *Oakwood University Chooses Dynamic Campus to Deliver "Next Level" Technology Support*, (June 12, 2019), *available at* https://dynamiccampus.com/6-12-19-oakwood-university-chooses-dynamic-campus-to-deliver-next-level-technology-support/.

25. Dynamic Campus promised and agreed to assign experts in the field to work on Oakwood's IT System, and specifically warranted that:

> [A]LL THE PROFESSIONAL STAFF IT ASSIGNS TO PERFORM THE SERVICES UNDER THIS AGREEMENT SHALL HAVE THE EDUCATION AND PROFESSIONAL EXPERIENCE REPRESENTED BY DYNAMIC CAMPUS AND BE COMPETENT TO PERFORM THE SERVICES RENDERED BY THEM IN THE PERFORMANCE OF THIS AGREEMENT. ***DYNAMIC CAMPUS SHALL ALSO PERFORM ITS SERVICES IN A GOOD AND WORKMANLIKE MANNER CONSISTENT WITH GOOD PROFESSIONAL STANDARDS AND IN COMPLIANCE WITH APPLICABLE LAWS***.

(*Id.* at 4) (emphasis added).

26. The Agreement also obligated Dynamic Campus to restore Oakwood's data or systems after a cyberattack or data loss within a commercially reasonable time:

> ***In the event of loss, damage, or destruction of any date [sic], or the inability of OU to use any service system or program due to the sole negligence of Dynamic Campus, Dynamic Campus shall take commercially reasonable steps to restore such data, service, system or program within a commercially reasonable period of time.*** The failure of Dynamic Campus to restore such data, service, system or program within a commercially reasonable time shall be deemed a material breach of this Agreement.

(*Id.*) (emphasis added).

27. The Agreement adopted and incorporated a lengthy "Statement of Work." This Statement describes the services Dynamic Campus would provide to Oakwood during the term of the Agreement.

28. Among other relevant provisions, the Statement of Work describes Dynamic Campus's obligation to ***"[p]rovide, refresh, restore, and backup services for optimal service***" and to "[***t]est the backups to ensure the systems can be restored properly from the backups and as required and in preparation for an unforeseen disaster***." (*Id.* at 17) (emphasis added).

29. The University relied upon Dynamic Campus's expertise as its "strategic technology partner," including Dynamic Campus's obligation to help prevent the risks of a ransomware attack, and/or prepare the University for an effective response to such an attack, and/or reduce the University's potential losses from such an attack.

The Ransomware Attack

30. In March 2022, a Threat Actor emailed an infected attachment to a person using an Oakwood email address. The available evidence after the attack demonstrated that someone opened the attachment.

31. In March 2022, the University detected unauthorized activity that impacted the availability and functionality of its computer systems.

32. More specifically, between March 7, 2022, and March 14, 2022, the Threat Actor accessed the University's internal systems, including personal and confidential information. Because of the acts and omissions of Dynamic Campus, the cyber criminals were able to access and lock Oakwood out of its vital IT systems,

and, perhaps even worse, Dynamic Campus was unable to provide timely backups to restore Oakwood's IT functions.

Dynamic Campus Caused or Contributed to the Attack

33. Dynamic Campus was not the entity that introduced ransomware or malware into its IT Systems. Nevertheless, DCS caused or contributed to the Attack as described in this Complaint.

34. The Threat Actor managed to introduce ransomware (or malware) into Oakwood's Email Server, and then access and control Oakwood's most vital IT Systems. The criminal was able to do this as a direct result of Dynamic Campus's fundamental failures to protect the systems and data from this very kind of attack.

35. Dynamic Campus caused/contributed to the ransomware attack in multiple ways, including:

- **Leaving the "Keys" in Plain Sight** - Dynamic Campus stored pass keys or passwords to vital programs/systems **in plain sight** (i.e., in a location easily accessible to and readable by a hacker). These indispensable "keys" were not encrypted or otherwise protected from view by an intruder into the University's IT Systems. Stated differently, Dynamic Campus put the "keys to Oakwood's kingdom" in a location that a hacker could easily access using ransomware. If Dynamic Campus had stored the keys in another

location or in a way that prevented a third party from seeing or accessing them (for example, storing them off-site or encrypting them), the hacker would not have been able to gain control over Oakwood's entire system.

- **Failure to Keep Fresh Data Backups in a Safe Location** – Dynamic Campus also failed to keep fresh backups in a secure location. Dynamic Campus chose to defy common sense by keeping Oakwood's backups in the same IT environment as the rest of its servers. As a result, when the hacker locked Oakwood out of its IT systems and data, the hacker also encrypted the passwords. If Dynamic Campus had maintained fresh backups of Oakwood's data in a safe location, in accordance with industry standards, Oakwood could have restored the backups on new servers, resumed normal operations in a short time and ended the cyber-event (and the University would not have had to pay the Threat Actor the steep ransom).

36. Dynamic Campus tries to explain away its malfeasance by blaming its failures on others. Specifically, Dynamic Campus blames Dell for DCS's failure to provide Oakwood with fresh data backups after the attack. Dynamic Campus claims that it had arranged for data backups in a safe location, on a Dell storage device

(called an "ExtremIO storage device"). DCS then blames Dell for damaging the storage device, thereby depriving Oakwood from receiving the backups supposedly kept on the device. This attempt to pin its failures on Dell fails for multiple reasons. In fact, the allegations effectively admit that DCS failed to live up to its obligations to keep fresh and accessible data backups.

37. Dynamic Campus had a duty (contractually and professionally) to keep Oakwood's backups in a location that could not be corrupted by ransomware or malware. Specifically, as noted above, DCS had a duty to"[***t]est the backups to ensure the systems can be restored properly from the backups and as required and in preparation for an unforeseen disaster***." (*Id.* at 17). DCS failed to do so.

38. Instead, Dynamic Campus completely relied on keeping Oakwood's data backups on a Dell storage device which was part of the same "ecosystem" as Oakwood's IT systems. In other words, a hacker could access the Dell storage device during a cyber-attack of Oakwood's primary operating systems. DCS knew or should have known that the data was at risk in such an attack and taken reasonable steps to eliminate the risk. For example, it could have encrypted the data on the Dell device or, even better, kept the Dell device in a different ecosystem such as an external (unconnected device) or a location in the "cloud." Failing to do so caused or contributed to the attack and Oakwood's damages.

39. Before the attack and during the response efforts, Dynamic Campus

representatives made false statements about available backups and suppressed the truth of the situation.

40. Despite repeated pleas for its data backups, Dynamic Campus did not produce any usable backups to Oakwood after the attack. Ultimately, Oakwood had to pay the hacker's ransom (**$804,000**), in order to regain access to IT systems and data, so that the University could try to resume the University's essential operations, serve its student community, and mitigate its damages.

Dynamic Campus's Failures Wreaked Havoc

41. Oakwood, its students and its employees suffered extensive damages from the ransomware as a direct result of Dynamic Campus's acts or omissions.

42. Oakwood staff dedicated countless hours working on data restoration and recovery efforts following the attack. Oakwood employees also had to perform many IT functions "manually" (in the absence of operational IT). For example, Oakwood staff had to manually process payrolls for several months, even after the threat actor returned control of Oakwood's core servers following the University's ransom payment.

43. The Threat Actor compromised student, patient, and employee data, which caused the University to incur legal fees notifying impacted individuals. Moreover, important student resources, such as transcripts, were unavailable until the end of May. This caused Oakwood students great anxiety, especially for students

who needed transcripts for entry into graduate and other educational programs.

44. Oakwood was subject to scrutiny from regulatory authorities such as the U.S. Department of Education ("DOE") following the Attack. The DOE placed the University on its watch list and required the University to provide a weekly status report about its systems to the DOE. Complying with strict federal reporting mandates alongside responding to community stakeholder concerns about data management and security only further depleted already limited University resources.

45. Oakwood is currently up for re-accreditation under the Southern Association of Colleges and Schools Commission on Colleges ("SACSCOC"). Cybersecurity is an explicit cornerstone of the re-accreditation process. Whether an "institution protects the security, confidentiality, and integrity of its student records and maintains security measures to protect and back up data" is considered one of the SACSCOC's Core Principles of Accreditation. Oakwood has not learned yet whether SACSCOC is going to make an adverse finding based on the cybersecurity event.

CAUSES OF ACTION

COUNT I — BREACH OF CONTRACT

46. Defendant re-alleges and reasserts the preceding factual allegations as if fully set forth herein.

47. Here, the parties entered into an Agreement. At all relevant times,

including before the Ransomware Attack, Oakwood had performed its obligations under the Agreement.

48. Dynamic Campus breached the Agreement and caused, contributed to, or was a causal factor in the ransomware attack by leaving the keys to Oakwood's IT systems in an area easily accessible to hackers and failing to ensure fresh backups were available to Oakwood.

49. As a result of Dynamic Campus's breach of the parties' Agreement, Oakwood suffered extensive damages, including being forced to pay a ransom to the Threat Actor and having to pay a massive cybersecurity premium increase due to, among other items, insurance claims made because of the Attack itself and Dynamic Campus's unsatisfactory management of Oakwood's cyber controls.

50. Oakwood also suffered from public and extensive reputational harm amongst its stakeholders and experienced significant additional labor costs due to Oakwood staff working long and unexpected hours to compensate for restoration delays caused by Dynamic Campus.

51. Oakwood demands judgment against Dynamic Campus in the form of compensatory damages and other further relief to which Defendant shows it is justly entitled at law or in equity as the jury deems fit.

COUNT II — NEGLIGENCE

52. Defendant re-alleges and reasserts the preceding factual allegations as

if fully set forth herein.

53. At all times herein mentioned, Oakwood acted in a reasonable, prudent manner.

54. Dynamic Campus owed Oakwood duties concerning its IT Systems. These duties included exercising reasonable care in ensuring the security of Oakwood's IT Systems and preparing the University to effectively and promptly respond to a cybersecurity event to eliminate or minimize the potential risks.

55. Dynamic Campus breached that duty by failing to act as a reasonable IT Systems professional and/or Shared Services Provider in various ways. For example, Dynamic Campus created or allowed the keys or passwords to Oakwood's vital IT systems and confidential and sensitive data in a location that was easily seen and accessed by the hacker's malware/ransomware. Dynamic Campus fundamentally violated its duty of care to Oakwood by: (1) leaving the keys/passwords to Oakwood's IT Systems and data "out in the open" (in a location easily seen and accessible by a hacker), (2) failing to store the keys/passwords in a completely different storage environment that a hacker could not have accessed (for example, on an external hard-drive or a separate location "in the cloud"), (3) failing to encrypt the keys/passwords and other sensitive data that were accessible by a hacker, and (4) failing to apply additional password or multi-factor protection to this data.

56. Dynamic Campus knew and could foresee that a Threat Actor could identify, read and access the keys/password after gaining access to Oakwood's Email Server, yet it utterly failed to protect such data from the foreseeable damage that a Threat Actor could wreak with access to that information.

57. Dynamic Campus also failed to discharge its duty of care to Oakwood by failing to set up regular and "fresh" data backups of Oakwood's vital IT Systems, testing the backups and storing them in a separate location, safe from a Threat Actor during a malware/ransomware attack.

58. Dynamic Campus knew and could foresee that failure to maintain fresh, safe and easily accessible data increased the risk of danger and damage from a Threat Actor's attack.

59. Oakwood suffered damages a direct and proximate result of Dynamic Campus' negligence, including compensatory damages, financial harm, and reputational injury.

60. Oakwood demands judgment against Dynamic Campus in the form of compensatory damages, and other and further relief to which Defendant shows it is justly entitled at law or in equity as the jury deems fit.

COUNT III —WANTONNESS

61. Defendant re-alleges and reasserts the preceding factual allegations as if fully set forth herein.

62. At all times herein mentioned, Oakwood acted in a reasonable, prudent manner.

63. Dynamic Campus had a duty to ensure the security of Oakwood's IT Systems.

64. Dynamic Campus recklessly and wantonly breached that duty by leaving the keys to Oakwood's IT systems in an easily accessible area and failing to ensure fresh backups were available to Oakwood.

65. Dynamic Campus knew that its wanton failure to properly secure Oakwood's IT systems and ensure the existence and security of quality backups increased the danger and damage of a ransomware attack.

66. As a direct and proximate result of Dynamic Campus's reckless and wanton conduct, Oakwood has suffered financial and reputational harm.

67. Oakwood demands judgment against Dynamic Campus in the form of compensatory damages, punitive damages, and other and further relief to which Defendant shows it is justly entitled at law or in equity as the jury deems fit.

COUNT IV — PROMISSORY FRAUD

68. Defendant re-alleges and reasserts the preceding factual allegations as

if fully set forth herein.

69. During the course of its business relationship with Oakwood, Dynamic Campus made false promises and misrepresentations of material fact that it had "optimal" backup services. Such backup services related to DCS's more general representations that it could respond adequately to a devastating event like the ransomware attack.

70. Dynamic Campus made these false promises and misrepresentations of material fact willfully to deceive Oakwood. At the time Dynamic Campus made its false promises and misrepresentations, it did not intend to perform the acts as promised.

71. Dynamic Campus's false promises and misrepresentations induced Oakwood to act or refrain from acting, including, without limitation: (a) ensuring Oakwood had another, alternative data backup service in case of a cybersecurity attack by a Threat Actor; and (b) refraining from requesting Dynamic Campus to ensure proper storage of necessary credentials and passwords related to Oakwood's backup servers.

72. Oakwood trusted that Dynamic Campus was dealing honestly and in good faith, and reasonably relied on and acted to its detriment because of Dynamic Campus's misrepresentations.

73. As a direct and proximate result of Dynamic Campus's promissory

fraud, Oakwood has suffered and will continue to suffer substantial damages.

74. Dynamic Campus's acts and omissions were undertaken with the intent to defraud. Agents of Dynamic Campus knew that its acts and omissions, as described herein, placed Oakwood in harm's way, but failed to address, correct or bring the risks to Oakwood's attention.

75. Oakwood demands judgment against Dynamic Campus in the form of compensatory damages, and other and further relief to which Defendant shows it is justly entitled at law or in equity as the jury deems fit.

COUNT V — FRAUDULENT SUPPRESSION

76. Defendant re-alleges and reasserts the preceding factual allegations as if fully set forth herein.

77. Dynamic Campus suppressed material information regarding its acts and omissions concerning data security and the fact that it was not making timely backups of Oakwood's servers and other data server backups before, during, and after the Attack.

78. Dynamic Campus owed a duty to Oakwood and was obligated to disclose these and other material facts to the University.

79. Dynamic Campus failed to disclose such issues to Oakwood University, which damaged Oakwood.

80. Oakwood trusted that Dynamic Campus dealt honestly and in good

faith. Oakwood reasonably relied on Dynamic Campus and entrusted management of its IT platform to Dynamic Campus, who acted to Oakwood's detriment.

81. As a direct and proximate result of Dynamic Campus's fraudulent suppression, Oakwood suffered and will continue to suffer damages.

82. Dynamic Campus took all these actions with the intent to defraud.

83. Oakwood demands judgment against Dynamic Campus in the form of compensatory damages, and other and further relief to which Defendant shows it is justly entitled at law or in equity as the jury deems fit.

COUNT VI — NEGLIGENT MISREPRESENTATION

84. Defendant re-alleges and reasserts the preceding factual allegations as if fully set forth herein.

85. Dynamic Campus recklessly or negligently misrepresented material information regarding Oakwood's IT systems before, during, and after the Attack.

86. Dynamic Campus knew or should have known the information it conveyed to Oakwood regarding its IT systems was false.

87. Dynamic Campus failed to exercise reasonable care in obtaining and in communicating the information regarding the IT platform to Oakwood.

88. Oakwood reasonably and justifiably relied on Dynamic Campus's misrepresentations by entrusting management of its IT platform to Dynamic Campus, who acted to Oakwood's detriment.

89. Oakwood would have attempted to take additional steps to protect itself, but for the misrepresentations of Dynamic Campus.

90. As a direct and proximate result of Dynamic Campus's misrepresentation, Oakwood suffered and will continue to suffer damages.

91. Oakwood demands judgment against Dynamic Campus in the form of compensatory damages, and other and further relief to which Defendant shows it is justly entitled at law or in equity as the jury deems fit.

PRAYER FOR RELIEF

92. WHEREFORE, premises considered, Oakwood respectfully requests that Plaintiff be summoned to appear and answer, and that upon final trial, the Court enter a judgment for Defendant and against Plaintiff as follows:

93. For actual damages, consequential damages, incidental damages, and punitive damages;

94. For pre-and-post-judgment interest;

95. For restitution and/or disgorgement of all ill-gotten benefits unjustly obtained and retained by Plaintiff;

96. For attorneys' and expert witness fees, court costs, and all other expenses associated with the prosecution of this action; and

97. For such other and further relief to which Defendant shows it is justly entitled at law or in equity.

Respectfully submitted:

/s/ David B. Block
David B. Block
One of the Attorneys for Oakwood University, Inc.

OF COUNSEL:
David B. Block
Reave W. Shewmake
BUTLER SNOW LLP
200 West Side Square, Suite 100
Huntsville, Alabama 35801
Telephone: (256) 551-0171
Fax: (256) 936-5650
David.Block@butlersnow.com
Reave.Shewmake@butlersnow.com

OF COUNSEL:
Margaret Loveman
BUTLER SNOW LLP
One Federal Place, Suite 1000
1819 5th Avenue North
Birmingham, Alabama 35203
Telephone: (205) 297-2200

CERTIFICATE OF SERVICE

This is to certify that on the 19th day of July 2023, the undersigned filed the foregoing using the Court's CM/ECF system, which will send notification of such filing to the appropriate CM/ECF participants as indicated on the filing receipt.

/s/ David B. Block
Of Counsel